

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-196664

(43)Date of publication of application : 14.07.2000

(51)Int.Cl.

H04L 12/56

(21)Application number : 11-268018

(71)Applicant : LUCENT TECHNOL INC

(22)Date of filing : 22.09.1999

(72)Inventor : DOSHI BHARAT TARACHAND
HERNANDEZ-VALENCIA ENRIQUE
SRIRAM KOTIKALAPUDI
WANG YUNG-TERNG
YUE ON-CHING

(30)Priority

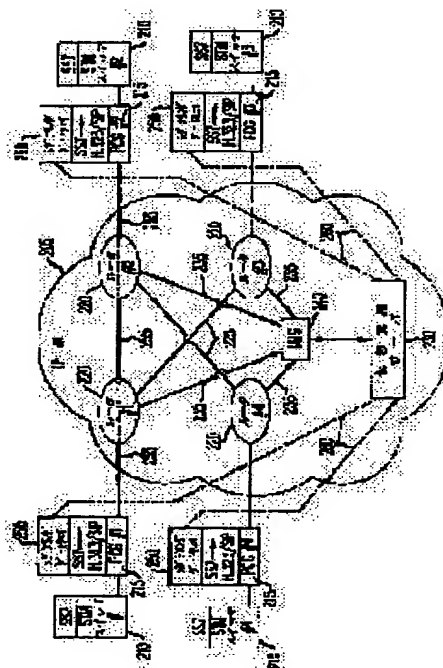
Priority number : 98 158694 Priority date : 22.09.1998 Priority country : US

(54) METHOD FOR PROVIDING SERVICE QUALITY FOR TRAFFIC SENSITIVE TO DELAY TRANSMITTED ON INTERNET NETWORK

(57)Abstract:

PROBLEM TO BE SOLVED: To insure service quality for IP network transmission traffic.

SOLUTION: An IP network path used for IP packet transmission between a transmission side edge device and a destination edge device is identified, and bandwidth is virtually supplied to voice traffic. It is secured to meet voice delay requirement of a high priority by allowing a connection request for a new voice call based on residual free capacity after giving a priority to a voice packet. Also, a VP server 230 maintains data about bandwidth capacity of each path segment in an IP network 205, the data of the bandwidth is supplied to a signaling gateway 250, it is allowed or rejected based on the quantity of empty bandwidth, and the decision of permission or rejection is notified to the transmission side edge device. Thus, guarantee about allowable delay and jitters can be attained without having to directly send a signal to respective IP routers constituting the IP network path.



Best Available Copy

LEGAL STATUS

[Date of request for examination] 27.12.2000

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision
of rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2000 Japanese Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-196664

(P2000-196664A)

(43) 公開日 平成12年7月14日 (2000.7.14)

(51) Int.Cl.⁷

H 0 4 L 12/56

識別記号

F I

H 0 4 L 11/20

テーマコード(参考)

1 0 2 E

審査請求 未請求 請求項の数20 O L (全 11 頁)

(21) 出願番号 特願平11-268018

(22) 出願日 平成11年9月22日 (1999.9.22)

(31) 優先権主張番号 09/158694

(32) 優先日 平成10年9月22日 (1998.9.22)

(33) 優先権主張国 米国 (US)

(71) 出願人 596092698

ルーセント テクノロジーズ インコーポ
レーテッド

アメリカ合衆国. 07974-0836 ニュージ
ャーシー, マレイ ヒル, マウンテン ア
ヴェニュー 600

(72) 発明者 プハラット クラチャンド ドシ

アメリカ合衆国 07733 ニュージャーク
イ, ホルムデル, デアボンド レーン 5

(74) 代理人 100064447

弁理士 岡部 正夫 (外11名)

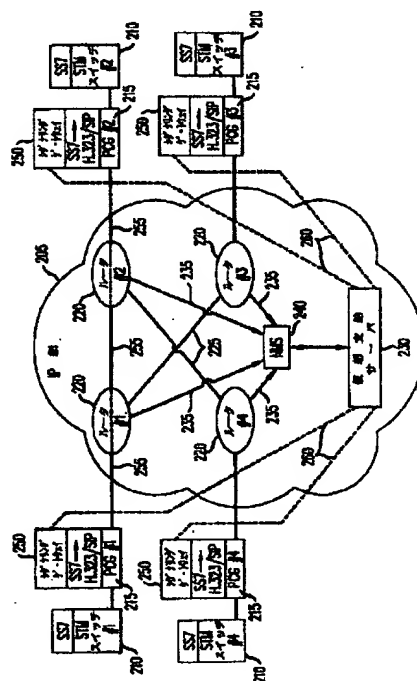
最終頁に続く

(54) 【発明の名称】 インターネット網上を伝送される遅延に敏感なトラヒックに対してサービスの品質を提供するための方法

(57) 【要約】 (修正有)

【課題】 IP網伝送トラヒックにサービス品質を保証する。

【解決手段】 発信側エッジデバイスと宛先エッジデバイスとの間のIPパケット伝送のために用いるIP網経路を識別し、帯域幅を音声トラヒックに対して仮想的に支給することで達成される。音声パケットに優先を与え、新たな音声呼の接続リクエストを、残された空いた容量に基づいて許可することで、高優先度の音声遅延要件を満たすことが確保される。VPサーバにて、IP網内の各経路セグメントの帯域幅容量に関するデータが維持され、帯域幅容量のデータがシグナリングゲートウェイに供給され、空いた帯域幅の量に基づいて許可あるいは拒絶する。許可あるいは拒絶の決定を発信側エッジデバイスに通知する。こうして、許容できる遅延およびジッタに関する保証が、IP網経路を形成する個々のIPルータに信号を直接に送る必要なしに達成される。



【特許請求の範囲】

【請求項1】 インターネット（IP網）内の経路上を運ばれる遅延に敏感なトラヒックに対してサービスの品質を保証するための方法であって、前記IP網が仮想プロビジョニングサーバ（VPサーバ）を備え、発信側エッジデバイスが前記IP網を通じての前記遅延に敏感なトラヒックの発射（伝送）のインタフェースとして機能し、この方法が：シグナリングゲートウェイの所で、前記経路に対する帯域幅容量を表す値を受信するステップ；前記シグナリングゲートウェイの所で、前記経路を通じて追加の遅延に敏感なトラヒック成分を設定するリクエストを受信するステップ；前記シグナリングゲートウェイの所で、前記経路の帯域幅容量を表す値と前記追加の遅延に敏感なトラヒック成分が前記経路を通じて接続された場合に必要とされる総帯域幅とを比較するステップ；および前記シグナリングゲートウェイの所で、前記必要とされる総帯域幅が前記経路の帯域幅容量を表す値より大きな場合、前記追加の遅延に敏感なトラヒック成分を接続するリクエストを拒絶する信号を生成するステップを含むことを特徴とする方法。

【請求項2】 前記経路の帯域幅容量を表す前記値が、前記VPサーバから前記シグナリングゲートウェイに送信されることを特徴とする請求項1の方法。

【請求項3】 前記経路を通じて前記追加の遅延に敏感なトラヒック成分を接続するリクエストが前記発信側エッジデバイスから搬送されることを特徴とする請求項1の方法。

【請求項4】 前記発信側エッジデバイスがパケット回路（PC）ゲートウェイであることを特徴とする請求項3の方法。

【請求項5】 さらに、前記追加の遅延に敏感なトラヒック成分を接続するリクエストを拒絶する信号を前記シグナリングゲートウェイから前記発信側エッジデバイスに搬送するステップを含むことを特徴とする請求項1の方法。

【請求項6】 さらに：前記シグナリングゲートウェイの所で、前記必要とされる総帯域幅が前記経路の帯域幅容量を表す値以下である場合、前記追加の遅延に敏感なトラヒック成分を接続するリクエストを許可する信号を生成するステップ；および前記追加の遅延に敏感なトラヒック成分を接続するリクエストを許可する信号を前記シグナリングゲートウェイから前記発信側エッジデバイスに送信する（運ぶ）ステップを含むことを特徴とする請求項1の方法。

【請求項7】 さらに、前記シグナリングゲートウェイが前記IP網内の複数の経路上の前記遅延に敏感なトラヒックの品質を監視および制御するステップを含み、前記IP網内の前記複数の経路が前記遅延に敏感なトラヒックを前記発信側エッジデバイスからの宛先エッジデバイスへ運ぶために用いられ、この方法がさらに：前記シグナ

リングゲートウェイの所で、前記IP網内の前記複数の経路の少なくとも一つの経路を、最も限られた利用可能な帯域幅容量を有するものとして識別するステップ；および前記発信側エッジデバイスから送出される前記遅延に敏感なトラヒックの量を前記最も限られた利用可能な帯域幅容量以下に制限するステップを含むことを特徴とする請求項1の方法。

【請求項8】 発信側パケット回路ゲートウェイ（PCゲートウェイ）と宛先PCゲートウェイとの間を複数のルータを含むIP網を通じて運ばれるリアルタイム音声伝送トラヒックのサービス品質を保証するための方法であって、前記発信側PCゲートウェイが前記IP網内を前記IP網の経路を通じて運ばれる前記リアルタイム音声伝送トラヒックを発射（伝送）するインタフェースとして機能し、

第一の仮想プライベート網に対する第一の帯域幅容量を前記IP網経路に関連する帯域容量から分割するステップを含み、前記仮想プライベート網が前記発信側PCゲートウェイと前記宛先PCゲートウェイとの間を運ばれる前記リアルタイム音声伝送トラヒックに対して契約され、この方法がさらにシグナリングゲートウェイの所で、前記第一の仮想プライベート網に対して支給された帯域幅容量を表す値を維持するステップ；前記シグナリングゲートウェイの所で、前記発信側PCゲートウェイから前記第一の仮想プライベート網を通じて前記宛先PCゲートウェイに向けて新たな呼接続を複数の現在既に確立されている呼接続に加えて確立するリクエストを受信するステップ；前記シグナリングゲートウェイの所で、前記第一の仮想プライベート網に対して支給された帯域幅容量を表す前記値と前記新たな呼接続が確立されたとき必要とされる前記第一の仮想プライベート網の帯域幅容量とを比較するステップ；前記シグナリングゲートウェイから、前記新たな呼接続が確立されたとき必要とされる前記第一の仮想プライベート網の前記帯域幅容量が前記第一の仮想プライベート網に対して支給された帯域幅容量を表す前記値より大きな場合、前記新たな呼接続を確立するリクエストを拒絶する信号を送信するステップを含むことを特徴とする方法。

【請求項9】 さらに：前記シグナリングゲートウェイから、前記新たな呼接続が確立されたとき必要とされる前記第一の仮想プライベート網の前記帯域幅容量が前記第一の仮想プライベート網に対して支給された帯域幅容量を表す前記値以下である場合、前記新たな呼接続を確立するリクエストを許可する信号を送信するステップを含むことを特徴とする請求項8の方法。

【請求項10】 仮想プロビジョニングサーバ（VPサーバ）が前記シグナリングゲートウェイに、前記第一の仮想プライベート網に対して支給された帯域幅容量を表す前記値を供給するために用いられることを特徴とする請求項8の方法。

【請求項11】 前記VPサーバが前記IP網の経路を通じての複数の仮想プライベート網を維持するように適合されることを特徴とする請求項10の方法。

【請求項12】 前記サービス品質保証が、前記発信側PCゲートウェイと宛先PCゲートウェイとの間を運ばれる前記リアルタイム音声伝送トラヒックの遅延を保証閾値以下に維持することに関することを特徴とする請求項8の方法。

【請求項13】 前記サービス保証が、前記発信側PCゲートウェイと宛先PCゲートウェイとの間を運ばれる前記リアルタイム音声伝送トラヒックのジッタを保証閾値以下に維持することに関することを特徴とする請求項8の方法。

【請求項14】 回路交換方式の網交換機が前記発信側PCゲートウェイからの前記複数の現在確立されている呼接続と前記新たな呼接続を伝送および終端するために用いられることを特徴とする請求項8の方法。

【請求項15】 前記回路交換方式の網交換機が、同期転送モード (STM) 交換機であることを特徴とする請求項14の方法。

【請求項16】 前記複数のルータの少なくとも一つのルータが、マルチ・プロトコル・スイッチング (MPLS) をサポートすることを特徴とする請求項8の方法。

【請求項17】 前記複数のMPLSルータが前記発信側PCゲートウェイと前記宛先PCゲートウェイとの間に複数の経路を設定するために用いられることを特徴とする請求項10の方法。

【請求項18】 前記VPサーバがさらに、前記シグナリングゲートウェイに、前記発信側PCゲートウェイと宛先PCゲートウェイとの間の前記複数の各経路の帯域幅容量を表す複数の値を供給することを特徴とする請求項10の方法。

【請求項19】 複数のVPサーバが対応する複数の開放最短ファーストドメイン (OSPF) ドメインを扱うために用いられることを特徴とする請求項10の方法。

【請求項20】 複数のVPサーバが対応する複数のマルチ管理エリアを扱うために用いられることを特徴とする請求項10の方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、IP網の分野、より詳細には、IP網を用いて遅延に敏感なトラヒックを輸送することに関する。

【0002】

【従来の技術】 音声サービス用のグローバルな網インフラストラクチャが、回路交換方式を用いて、公衆電話網 (PST) や構内交換 (Private Branch Exchange, PBX) 網によってサポートされている。これら網は、呼接続の確立のためや、網スイッチの所のルーティングマップのために、シグナリングを用いる (制御情報の送信を行な

う)。呼接続の確立の際に制御信号が送信されるために、個々の交換機は、新たな呼接続をサポートするための空いた帯域幅が無い場合は、呼接続のリクエストを拒絶することができる。このように、接続経路内の全ての交換機が空いた帯域幅が無いときは、新たな呼接続のリクエストを拒絶できるために、回路交換方式の音声網では、確立された接続に対してサービスの品質 (QoS) を保証することができる。回路交換方式の音声網においては、QoSは、新たな呼接続の試みを拒絶する方が、呼を新たに接続することで接続された呼の性能が劣化されることより好ましいという基本理念の下で保証される。

【0003】 IPベースのイントラネットや公衆インターネットの爆発的な成長の結果として、IPベースのルータの大規模な網インフラストラクチャが形成されつつある。近年は、この大規模なIP網インフラストラクチャが音声を実タイムに伝送するためのビークル (乗り物) として用いられるようになってきた。これはインターネット電話としても知られているが、このインターネット電話の電話市場におけるシェアは増大の一途にある。

【0004】

【発明が解決しようとする課題】 ただし、回路交換音声サービス網の場合とは異なり、IP網内に含まれるルータには制御信号は送信されない。IP網においては、ソース (発信元)、宛先、および中間ルータの間で制御信号の通信が行なわれないために、IPルータの所では、新たな呼を、結果としてそのルータの帯域幅容量を超える場合でも拒絶することはできない。このため、インターネットを用いてのリアルタイム伝送では、公衆網 (PSTN) や構内交換機 (PBX) ではあまり問題とならない遅延とジッタの問題が発生する。より具体的には、インターネットや他のIP網を用いての伝送は、最善努力伝送モードにて達成され、このため、IP網を用いての電話は、現時点では、音声や他の遅延に敏感な伝送のQoS (サービスの品質) を保証することはできない。

【0005】

【課題を解決するための手段】 本発明によると、インターネットプロトコル (IP) 網上を伝送される音声や他の遅延に敏感な伝送に対するQoS (サービスの品質) の保証は、発信側エッジデバイスと宛先エッジデバイスとの間のIPパケット伝送のために用いるIP網経路を識別し、IP網経路の帯域幅を音声トラヒックに対して仮想的にプロビジョニング (割り当てる) ことで達成される。音声パケットに優先を与え、新たな音声呼 (および他の遅延に敏感なトラヒック) の接続リクエストを、そのIP網経路上に残された空いた容量に基づいて許可することで、高優先度の音声 (および他の遅延に敏感なトラヒック) が厳しい遅延要件を満たすことが確保される。仮想支給サーバ (VPサーバ) を用いて、IP網内の各経路セグメントの帯域幅容量に関するデータが維持され、帯域幅容量

のデータがシグナリングゲートウェイに供給される。シグナリングゲートウェイは追加の遅延に敏感なトラヒック成分の接続をIP網経路の空いた帯域幅の量に基づいて許可あるいは拒絶する。次に、シグナリングゲートウェイは、この許可あるいは拒絶の決定を発信側エッジデバイスに通知する。こうして、QoSの保証、つまり、IP網を用いてのリアルタイム伝送に対して許容できる遅延およびジッタに関する保証が、IP網経路を形成する個々のIPルータに信号を直接に送る必要なしに達成される。以下では、本発明のより完全な理解を期するために、本発明を図面を用いて説明する。

【0006】

【発明の実施の形態】図1、2、および3は、本発明による仮想支給サーバ（VPサーバ）230を利用するパケット回路ゲートウェイ（PCゲートウェイ）エッジデバイス215間のIP網205の様々な実施例を示す。図1においては、VPサーバ230は、各PCゲートウェイエッジデバイス215と関連するシグナリングゲートウェイ250と通信する。図2においては、VPサーバ230は、一つのPCゲートウェイ215と同一位置に配置されたシグナリングゲートウェイ250と通信し、このシグナリングゲートウェイ250により、網内の一つ以上の複数のPCゲートウェイ215に対するシグナリングゲートウェイ機能が遂行される。図3においては、VPサーバ230は、仮想プライベート網資源マネージャとしての追加の機能も遂行する。

【0007】本発明は、以下では、音声呼が、通常のPS TN（Public Switched Telephone Network：公衆網）回路スイッチ、例えば、STM（Synchronous Transfer Mode：同期転送モード）スイッチ210から発信され、IP網205内のルータ間の経路を用いて運ばれ、再び通常の回路スイッチに終端するような環境において用いるものとして説明される。ただし、当業者においては明らかなように、これら回路スイッチは、単純なアクセスマルチプレクサあるいはエッジビークルとして実現することもできる。加えて、本発明は、遅延に敏感なIPデータグラムトラヒックの輸送に用いた場合に最も効果的であるが、ただし、本発明は（音声トラヒックに加えて）他の任意のIPデータグラムトラヒックに対して用いることができる。回路スイッチ信号フォーマットからIPフォーマットへの変換が、SAC（Service Access Concentrator）あるいはITG（Internet Telephone Gateways）としても知られているPCゲートウェイ215の所で行なわれる。PCゲートウェイ215は、回路スイッチ信号フォーマットとIPフォーマットとの間の変換を遂行することに加え、音声の圧縮／圧縮解除、サイレンスの抑圧／挿入の他、特定の用途に対して必要とされる他の周知の機能を遂行する。

【0008】シグナリングゲートウェイ250は、シグナリング機構間の適当なインタフェースおよびインター

ワーキングの遂行に加え、関連するPCゲートウェイから発信された新たな呼リクエストの許可／拒絶の決定に用いられる。PSTN（公衆網）等の回路スイッチ網は、典型的には、接続の設定／切断に対するリクエストを送信するために、シグナリングシステム7（SS7）を用い、他方、IPのエンドポイントや中間ルータは、セッション管理のために、ITU-T H.323あるいはセッション開始プロトコル（SIP）を用いる。このために、シグナリングゲートウェイ250が、PCゲートウェイ215の所で遂行されるPSTN網とIP網205の間のシグナリング機構間の変換のための上位プロトコルとして用いられる。必ずしも、個々のPCゲートウェイ215の所に常駐のシグナリングゲートウェイ250が要求される訳ではなく、全てのPCゲートウェイに対するシグナリングゲートウェイ機能を単一の箇所に実現し、この単一のシグナリングゲートウェイから対応するPCゲートウェイ215に制御信号を送ることもできることに注意する。例えば、図1と図3は、個々のPCゲートウェイ215が常駐のシグナリングゲートウェイ250を維持する本発明の実施例を示し、図2は、一つのPCゲートウェイ、例えば、PCG#1のみが常駐のシグナリングゲートウェイ250を維持する実施例を示す。図2の実施例では、他のPCゲートウェイ、例えば、PCG#2、PCG#3、PCG#4に対するシグナリングゲートウェイ機能は、PCG#1の所に常駐するシグナリングゲートウェイから適当な制御信号をこれら残りの各PCゲートウェイに伝送することで提供される。この制御信号の伝送は、TCP/IPセッション内のサービスされているIP網205を用いて行なうことも、補助の伝送媒体を用いて行なうことも、あるいはデータ輸送のための任意の他の周知の手段を用いて行なうこともできる。

【0009】本発明の一つの新規な特徴はVPサーバ230が利用されるところにある。VPサーバ230は、シグナリングゲートウェイ250に、網の帯域幅容量に関する情報を供給するために用いられる。シグナリングゲートウェイ250は、この情報を用いて、関連するPCゲートウェイ215の所で新たな呼リクエストを許可すべきか、拒絶すべきかの決定を行なう。新たな呼に対する許可／拒絶の決定のための基準は、遅延、ジッタ、呼接続の損失などのQoS特性が確立された音声呼接続に対して保証閾値以下に維持されるように設定される。

【0010】VPサーバ230は、網帯域幅容量の情報を、シグナリングゲートウェイ250に、少なくとも一度、網動作の開始時に送信し、その後、リンクの障害、新たなリンクの確立、現存のリンクへの帯域幅の追加などのために下位のIP網リンクに帯域幅の変化が生じた場合に、必要に応じてこれを送信する。典型的には、IP網と関連して、網管理システム（NMS）240が存在する。NMS240の機能は当分野において周知であるが、ただし、本発明との関連では、NMS240は、VPサーバ230に、上述のリンク帯域幅の変化を通知する追加の

機能を遂行する。

【0011】図1～3には、PCゲートウェイ、例えば、PCG#1とPCG#2との間でのIPパケットの輸送のための網経路255が示される。経路255は、中間要素であるルータ220、例えば、ルータ#1とルータ#2を経由する。ルータ220は、IP網205の物理層において複数の物理層ルータ輸送セグメント225によって相互接続されている。説明の網経路255は、複数のこれら物理層ルータ輸送セグメント225を用いて確立される。網経路255は、これら複数の物理層ルータ輸送セグメント225を用いて確立される複数の経路リンクから成る。VPサーバ230は、シグナリングゲートウェイ250によって実現されるPSTNのプロビジョニング（割り当て）機能および許可制御と協力して、音声トラヒックに対して品質を保証することに加え、IP網内の残された容量を周知の最善努力モードを用いる他のトラヒックに割り当てる。類似のプロビジョニング（割り当て）により、サービスの保証を複数のクラスのトラヒック、例えば、ビデオ会議にも拡張することもできる。

【0012】特定のSTMスイッチ210が対応するPCゲートウェイ215に接続されているものとする。音声呼送能力は、従来のトラヒックエンジニアリング技法を用いて、ペアのPCゲートウェイ215の間で必要とされる容量を決定することで容易に予測できる。各ペアのPCゲートウェイ215の間の網経路の帯域幅要件は、例えば、使用される圧縮方式のタイプやサイレンス抑圧能力などの特定のフォーマット変数に依存して決まる。VPサーバ230は、IP網ルータ220と、これらルータ220の間の物理層ルータ輸送セグメント225の伝送能力（容量）に関するデータを維持管理する。本発明によると、VPサーバ230を用いて、IP網ルータ220の間の各経路によってペアのPCゲートウェイ215の間に必要とされる帯域幅要件を満たすために要求される容量が決定される。ルータ220や物理層ルータ輸送セグメント225などの各網要素によって要求される帯域幅は、遅延に敏感なトラヒックに対して利用できる（指定される）帯域幅容量の範囲内で仮想的に支給される（プロビジョニングされる）。本発明によると、帯域幅の割り当ては、新たに接続される呼の許可／拒絶が個々のルータ220の所で制御されるのではなく、PCゲートウェイエッジデバイス215の所で制御されるという意味において、仮想的に、支給される。PCゲートウェイ215の所で遅延に敏感な音声フレームあるいはIPパケットに対して帯域幅を支給された後に余った網要素上の帯域幅が遅延に強いパケットの輸送に用いられる。別の方法として、各IP網経路の最小限の帯域幅容量を遅延に強いトラヒックに対して支給しておき、残りの帯域幅を遅延に敏感なトラヒックに対して支給することもできる。IPパケットヘッダ内のTOS(Type-of-Service) フィールドを用いて、遅延に敏感なトラヒックタイプと遅延に強いトラ

ヒックタイプとが識別される。こうして、音声パケットにデータパケットより高い優先が与えることで、遅延およびパケットの損失の面でサービスの品質要件(QoS要件)が満たされることが保証される。

【0013】IP網ルータ220と特定の経路255のために用いられる物理層輸送セグメント225が、決定された（要求される）容量要件を満たすために必要とされる帯域幅容量を持たない場合は、VPサーバ230は、ボトルネック容量の部分はこの容量を求めて競合するペアのPCゲートウェイ215に割り当てた上で、関連するシグナリングゲートウェイ250にこの割り当てについて通知する。VPサーバ230は、さらに、現在および将来予測される帯域幅需要を満たすためにIP網205に追加することを必要とされる容量を計算する。こうして、VPサーバ230を用いて、中央で、要求される網帯域幅のプロビジョニング（割り当て）を計算および決定し、この帯域幅の割り当てをIP網205内のシグナリングゲートウェイ250に通知することで、シグナリングゲートウェイ250は任意のペアのPCゲートウェイ215の間で同時にサポートすることが可能な音声呼の最大個数を決定することが可能となる。シグナリングゲートウェイ250はSS7とH.323/SIPとの間のシグナリングインターワーキング機能も遂行し、このため、これらもペアのPCゲートウェイ215の間で進行中の接続された呼の個数を追跡することができる。図2に示す本発明の実施例においては、上述のように、一つのシグナリングゲートウェイ250を用いて複数のPCゲートウェイ215が制御されるが、この場合は、このシグナリングゲートウェイ250は、他のPCゲートウェイ215（図2の実施例ではPCG#2、PCG#3、PCG#4）の間で進行中の接続された呼の個数も追跡するためにも用いられる。

【0014】上述のように、VPサーバ230は、さらに、NMS240との間でもデータを交換する。NMS240は、IP網205の網要素の容量、網の帯域幅と容量需要、成長データ、リンク障害などに関する情報を維持するために用いられる周知の網コントローラである。NMS240は、網ルータ220とメッセージおよび信号を交換し、シグナリングチャンネル235を介してこの網情報を供給および維持する。ただし、NMS240は、PCゲートウェイ215の所での新たな呼の接続に対する許可／拒絶の決定を制御あるいは管理することはない。NMS240は、IP網205のトポロジ、容量、障害事象などに関する情報をVPサーバ230に供給し、VPサーバ230は、この情報を用いて自身の計算値を更新し、IP網内でルーティングアルゴリズムの重みの更新などの変更が必要とされる場合は、これをNMS240に通知する。ルーティングアルゴリズムの重みは、IPパケットを転送するためのルーティング経路の決定に用いられる。ルーティングアルゴリズムの重みの使用および実現は、IPネットワークワーキングの分野においては周知である。障害事象が原

因で必要な容量を一時的に満たすことができない場合は、VPサーバ230は、網内の障害の影響を受ける経路上でサポートすることができる呼の最大数を決定し、これを関連するシグナリングゲートウェイ250に通知し、これによって様々な網PCゲートウェイエッジデバイス215の所で接続される呼の個数が絞られる。

【0015】本発明の説明の実施例は、PSTNスイッチとシグナリングゲートウェイ250との間の接続の際のシグナリングの変換および許可制御を管理する背景で説明されたが、本発明は、PC（パケット回路）網の間で電話をサポートするためや、PSTNスイッチを介してPC網と電話網との間で電話をサポートするために用いることもできる。これら接続に対して接続品質を保証するためには、VPサーバ230からシグナリングゲートウェイ250にメッセージを送ることで、シグナリングゲートウェイ250に対して、PSTNとPC網から発信される電話トラヒックのために、PCG・ツウ・PCG経路によって必要とされる最小限の呼容量について通知する必要がある。加えて、この場合、つまり、呼がPC網から発信された場合は、網のオペレータによってコーディング速度は制御されないために、PC（パケット回路）ゲートウェイの所でトラヒックポリシー機能を用いて、呼設定シグナリングにおいて示されるトラヒック想定との合致を監視する必要がある。

【0016】PC（パケット回路）網から発信される音声呼にはPSTN（公衆網）から発信される音声呼より低い優先度を割って、シグナリングゲートウェイ250を介して、空いている帯域幅が少ない場合は、PCから発信された呼は拒絶し、PSTNから発信された呼を優先させることも考えられる。こうして、シグナリングゲートウェイ250を介してPCゲートウェイ230の所での呼の許可管理を強化すること、すなわち、PSTNから発信される音声サービスに他のサービスより高い優先度を与えることで、音声および他のQoSに敏感なサービスに対して、呼の接続品質を保証することができる。加えて、サービスプロバイダの立場から顧客に複数のクリティカルサービス保証を提供することや、顧客の立場から、複数の顧客がIP網205内の共通の経路上で類似のクリティカルサービス保証を要求することも考えられる。一例として、音声トラヒックに対する仮想プライベート網（Virtual Private Networks）を実現することもできる。つまり、網プロバイダが異なる位置の企業ユーザを相互接続するためのワイドエリアサービスを提供することもできる。複数の仮想プライベート網を公衆サービスと平行して共通のインフラストラクチャを用いて提供できる能力は、サービスプロバイダと企業顧客の両方にとって魅力的である。サービスプロバイダの立場からは、仮想プライベート網を提供することの利点として、第一に、ユーザに安全なアクセスを提供することができ、第二に、構内交換機（例えば、PBX）間のリースのプライベート回線の

それに匹敵するQoSを保証することができる。

【0017】仮想プライベート網の顧客は、ワイドエリア網オペレータあるいはサービスプロバイダから提供される帯域幅とサービス品質の保証について協議する。網オペレータは、こうして協議されたサービスのレベルを共通のインフラストラクチャを用いて全ての仮想プライベート網の顧客に対して保証し、これによって多重化利得を達成する。VPサービス230は、現在空いているルータ220の現在空いている容量を用いて、保証されたサービスの品質を提供する。例えば、今日では、ポート、ソース、および宛先識別に基づいてフローを識別し、保証されるべき協議されたサービスのレベルと帯域幅に基づいて一群のフローを複数のクラスおよび／あるいはスーパークラスに分けることができるルータが存在する。

【0018】これらルータは、加えて、各クラス、スーパークラスなどに対する最小および最大の帯域幅を割り当ておよび管理することもできる。これらルータの所にバッファとキューを管理する機構を組み込むことで、フローをクラスおよびスーパークラスに従って別個に異なる優先度にて扱うこともできる。加えて、あるクラス内の様々なフローおよび／あるいはあるスーパークラス内の様々なクラスの多重化を統計的に扱うこともできる。例えば、重み付け公平キューイングWFQ（Weighted Fair Queuing）サービスのシステムを用いて、フロー、クラス、およびスーパークラスの帯域幅の管理を行なうこともできる。クラスあるいはスーパークラスの一つが協議帯域幅割当てを超えた場合でも、他の協議クラスあるいはスーパークラスがそれらに割当てられた帯域幅を完全には使用していない場合、優れたサービス品質を提供することができる。こうして、協議された帯域幅割当てを超えるクラスあるいはスーパークラスに提供されるQoSのみが影響を受ける。

【0019】図3においては、VPサーバ230は、仮想プライベート網資源マネージャ（VPNRM）として用いられる。仮想プライベート網資源マネージャは、最適化アルゴリズムを利用することで、（1）顧客がサービスのさらなるクラス分けを希望する場合は、仮想プライベート網間および仮想プライベート網内の帯域幅の分割を行なうことに加え、（2）網内のフローのルーティングを制御する。利用されているルータ220がフロー分割機能は備えるが、フレキシブルルーティング機能は備えない場合は、フローのルートはIP網205内で固定され、IP網内の容量は、仮想プライベート網資源マネージャによって、協議された仮想プライベート網契約に基づいて分割される。VPサービス230は、仮想プライベート網資源マネージャとして機能し、この分割情報をIP網205内の個々のルータ220に送信し、網ルータ220は、この情報を用いて、アルゴリズムの重み、最小帯域幅、最大帯域幅、バッファ閾値等を設定する。仮想プラ

イベント網資源マネージャとの各ルータとの間の通信が、図3に、VPサーバ230と個々のルータとの間の仮想プライベート網シグナリング経路270として示される。図3に示す仮想プライベート網シグナリング経路270は、単に、解説のためのものであり、当業者においては明らかなように、ルータ220へのシグナリングのために他の複数の任意の手段を用いることもでき、例えば、NMS（網管理システム）240を用いてこれを行なうこともできる。いったん、網ルータ220の所に分割情報が受信され、分割が遂行されると、各仮想プライベート網がそれらに割り当てられた最小帯域幅を用いて確立される。

【0020】図1～3に再び戻り、音声に対する仮想プライベート網を、上述のように、アクセスビークルとしてPSTN（公衆網）スイッチあるいはマルチプレクサ（説明の例では、STMスイッチ210）を用い、バックボーンとしてIP網205を利用してサポートすることもできる。長所として、音声に対する仮想プライベート網を確立するためのこの実施例は、単純な優先機構を備えた網ルータ220を用いて達成することができる。つまり、この実施例では、仮想プライベート網を確立および維持するために、VPサーバ230と網ルータ220の間にはシグナリングは必要とされない。代わりに、VPサーバ230は、ペアのゲートウェイによって仮想プロビジョニング（仮想割当て）を遂行するために要求される総容量を使用（計算）する。仮想プライベート網の顧客からの新たな呼の許可／拒絶の制御は、VPサーバ230内に常駐する許可／拒絶アルゴリズムを利用し、シグナリングゲートウェイ250を介して、PCゲートウェイ215によって遂行される。

【0021】図4および図5は、PC（パケット回路）ゲートウェイ215の間に確立された仮想プライベート網上の新たな呼の許可／拒絶を遂行するための本発明による一例としてのアルゴリズムを示す。以下の説明においては、以下のような定義を用いる：

C = 総リンク帯域幅（310）

W = 利用可能ビット速度（ABR）あるいは最善努力データサービスを用いてサポートされる結合（総）トラヒックに対して常に利用できる最小帯域幅（315）

$C - W$ = 呼管理制御の目的で利用される総帯域幅（320）

$C - W - D_1$ = 呼管理制御の目的に対する上限閾値（325）

$C - W - D_2$ = 呼管理制御の目的に対する下限閾値（325）

$B_i(n_i)$ = 指定されるQoSを持つ仮想プライベート網VPN_iに対して n_i 個の接続をサポートするために必要な帯域幅

P_i = 仮想プライベート網VPN_iに対して契約された最小帯域幅

Q_i = 仮想プライベート網VPN_iに対して契約された最大帯域幅

k = 考慮下のリンクを共有するQoS保証を持つ仮想プライベート網の数

【0022】仮想プライベート網VPN_iに対する新たな呼の設定リクエストがシグナリングゲートウェイ250の所に到着すると、新たな呼を許可すべきか拒絶すべきかを決定するための図5に示す一例としてのアルゴリズムがステップ350から遂行される。 K 個の仮想プライベート網（VPN_i；ここで、 $i = 1, 2, 3, \dots, K$ ）によって用いられている帯域幅がシグナリングゲートウェイ250の所でモニタされる。ステップ355において、追加の呼をサポートするために要求される仮想プライベート網VPN_iの帯域幅が最大帯域幅割り当て（ Q_i ）を超える場合は、リクエストされた新たな呼は拒絶される。他方、追加の呼をサポートするために要求とされる仮想プライベート網VPN_iの帯域幅が最大帯域幅割り当て（ Q_i ）を超えない場合は、次に、ステップ360が遂行される。ステップ360において、仮想プライベート網VPN_iの帯域幅使用量が新たな呼を接続した後に、 $0 \sim (C - W - D_2)$ のレンジ以内になることが予測される場合は、新たな呼は許可される。他方、仮想プライベート網VPN_iの帯域幅使用量が（ $C - W - D_2$ ）より大きくなることが予測される場合は、次に、ステップ365が遂行される。ステップ365において、仮想プライベート網VPN_iの帯域幅使用量が（ $C - W - D_1$ ）から（ $C - W$ ）のレンジの間となることが予測される場合は、仮想プライベート網VPN_iに対する新たな呼の設定のリクエストは、ステップ370において、仮想プライベート網VPN_iによる帯域幅使用量がその最小割り当てを超えない場合に限り許可され、超える場合は拒絶される。他方、仮想プライベート網VPN_iの帯域幅使用量が（ $C - W - D_2$ ）から（ $C - W - D_1$ ）のレンジの間となることが予測される場合は、仮想プライベート網VPN_iに対する新たな呼の設定のリクエストは、ステップ375において、スライディングスケールアルゴリズムに基づいて確率的に許可あるいは拒絶される。 $q = (1 - \rho)$ は、下限閾値（ $C - W - D_2$ ）を超える帯域幅使用量を（ $D_2 - D_1$ ）で割った比であるものとする。ステップ380において、この確率ベースのアルゴリズムをサポートするために、シグナリングゲートウェイ250の所で乱数が生成される。ステップ385において、 x の値が確率 ρ 以下である場合は、新たな呼は許可される。呼が発信側PCゲートウェイと宛先PCゲートウェイとの間で複数のリンクを経由する場合は、呼が確立に当たって、図4および図5のアルゴリズムが各経路リンクに対して反復され、呼は、このアルゴリズムが経路内の各リンクに対して（呼を許可する）肯定的な決定を示した場合に限って、発信側PCゲートウェイと宛先PCゲートウェイとの間で接続される。

【0023】図5の一例としてのアルゴリズムを実現する際は、仮想プライベート網VPN_i上の呼の個数 N_i の関数としての帯域幅利用データ $B_i(n_i)$ が利用される。呼あるいは接続が定ビット速度の場合は、 $B_i(n_i)$ は、 n_i の単純な線形関数となる。ただし、呼あるいは接続が、本質的に、あるいは設計上、可変ビット速度である場合、例えば、サイレンスを除去された音声や、オン/オフデータ源等である場合は、 $B_i(n_i)$ は、典型的には、 n_i の非線形関数となる。 $B_i(n_i)$ の非線形性は、当分野において周知のように、ランダムに変化する可変ビット速度ソースを統計的にマルチプレキシングすることに起因する。パケット音声マルチプレキシングの背景での $B_i(n_i)$ 関数の具体的な性質については、例えば、K.Siram and Y.T.Wangによる論文“Voice Over ATM Using AAL2 and Bit Dropping: Performance and Call Admission Control”, Proceedings of the IEEE ATM Workshop, May 1998, pp. 215224において詳細に述べられているために、これを参照されたい。

【0024】VP（仮想プロビジョニング）サーバに関する上述の説明は、複数の相互接続されたOpen Shortest Path First (OSPF) ドメインを含むIP網の背景でなされた。ただし、本発明は、IP網が複数の相互接続された管理エリアから成り、各管理エリアが複数のOSPFドメインから成る場合にも適用できる。典型的には、各管理エリアは、必ずしも必須ではないが、個々のインターネットサービスプロバイダあるいはキャリアに属するIP網から成る。本発明のこのような一つの実施例においては、各管理エリアに、一つのゲートウェイVPサーバが設置され、各VPサーバは、これも本発明の必須要件ではないが、各管理エリアのゲートウェイルータと同一位置に設置される。各ベアの各ゲートウェイVPサーバは、自身の担当するベアのゲートウェイルータの間に必要とされる容量要件を決定する。加えて、各ゲートウェイVPサーバは、ベアの隣接する管理エリアの間に必要とされる帯域幅容量に関する情報を自身の管理エリア内の各OSPFドメイン内に位置するVPサーバに供給する。こうして、大きなIP網内の様々な箇所に位置するシグナリングゲートウェイに呼の許可/拒絶に対して必要とされる十分に情報が供給され、ある管理エリアから発信され別の管理エリアに終端する呼も同様に管理される。

【0025】上述の説明から明らかなように、本発明の様々な修正および代替の実現が可能である。例えば、上に説明の実施例では、単一のVPサーバが用いられ、これによって、IP網全体が扱われ、IP網内の全てのシグナリングゲートウェイが制御された。ただし、本発明は、多ドメイン動作に対して用いることもできる。つまり、呼の発信側が第一のIPドメインに接続された第一の電話ゲートウェイであり、呼の宛先が、もう一つのIPドメインを通じて接続された第二の電話ゲートウェイである場合、呼の処理には、第一のドメイン内のゲートウェイ

ルータへのドメイン内ルーティング、中間領域内のゲートウェイルータ間のルーティング、およびこのゲートウェイルータから最後のドメイン内の電話ゲートウェイへのドメイン内ルーティングが必要となる。この場合、一つの実現として、ドメイン内のルーティングの決定には、OSPF等のプロトコルを用い、ゲートウェイドメイン間のドメイン間ルーティングには、Border Gateway Protocol (BGP) を用いることが考えられる。本発明のこのような実施例においては、各IPドメインに対して1つずつ、全体では、複数のVPサーバが用いられる。各VPサーバは、自身のドメイン内のルータの仮想支給（プロビジョニング）をゲートウェイ境界ルータ（Gateway Border Router）のそれも含めて管理する。加えて、各ベアのインタフェーシングVPサーバは、自身の各ベアのインタフェーシングゲートウェイ境界ルータ間の容量要件も決定する。本発明の単一ドメイン実現の場合と同様に、発信側PCゲートウェイと宛先PCゲートウェイにおける呼の許可/拒絶の制御は、これら様々なルータに直接に信号を送ることなく行なわれる。本発明の多ドメイン実現においては、この機能は、様々なインタフェースされるVPサーバの間でドメイン内およびドメイン間ルーティングプロトコルを共有して用いることと、ルータアルゴリズムに静的な重みを与えることで達成される。

【0026】加えて、上に説明の実施例では、サービス品質の保証は、ルータと関連するVPサーバ（仮想プロビジョニングサーバ）の間にシグナリング機構を追加することなく達成されたが、本発明は、VPサーバから網ルータに直接に信号を送るようにすることもできる。ただし、このような実現では、プロビジョニング（割り当て）が対応する発信側ゲートウェイと宛先ゲートウェイの所ではなく、ルータの所で制御されるために、より正確には、このサーバは、仮想的にはなく、リアル（現実）にプロビジョニング（割り当て）を遂行するとな見做すことができる。この代替実施例では、OSPF (Open Shortest Path First) およびBGP (Border Gateway Protocol) における状態交換プロトコルが用いられ、これらが動的なトポロジーおよび容量情報を供給するように拡張される。

【0027】本発明は、さらに、網IPルータの所に周知のMPLS (Multi-Protocol Label Switching) が用いられる新に出現中のIP網内で用いることもできる。このようなMPLSベースのIP網においては、VPサーバによって、発信側と宛先のベアPCゲートウェイエッジデバイスの間の可能な複数の経路に関する情報が維持される。シグナリングゲートウェイは、VPサーバから、ベアのPCゲートウェイの間の様々な代替経路とその容量に関する情報を受信し、新たな音声呼のリクエストを、空いた任意の経路上に空いた容量が有る場合は、許可し、無い場合は、その呼リクエストを拒絶する。

【0028】このように、上述の説明は、単に解説のた

め、および当業者に本発明を遂行するための最良の形態を示すためのもので、本発明の全ての可能な形態を示すことを目的とするものではない。さらに、使用された用語（ワード）は、限定のためのではなく、解説のためのものであり、構造の細部については、本発明の精神から逸脱することなく実質的に変更が可能であり、特許請求の範囲に包含される全ての修正の排他的な使用が保護されるものである。

【図面の簡単な説明】

【図1】本発明によるペアのPCゲートウェイエッジデバイス間で、VPサーバを用いて、IP網を通じて、音声を送信するための一つの実施例であって、VPサーバが、複数のシグナリングゲートウェイと通信する実施例を示す図である。

【図2】本発明によるペアのPCゲートウェイエッジデバイス間で、VPサーバを用いて、IP網を通じて、音声を送信するためのもう一つの実施例であってVPサーバが、一つのPCゲートウェイと同一位置に配置されたシグナリングゲートウェイと通信し、この単一のシグナリングゲートウェイが、IP網内の複数のPCゲートウェイ215にシグナリングゲートウェイ機能を提供する実施例を示す図である。

【図3】本発明によるペアのPCゲートウェイエッジデバイス間で、VPサーバを用いて、IP網を通じて、音声を送

送するためのもう一つの実施例であって、VPサーバが、仮想プライベート網資源マネージャとしても機能する実施例を示す図である。

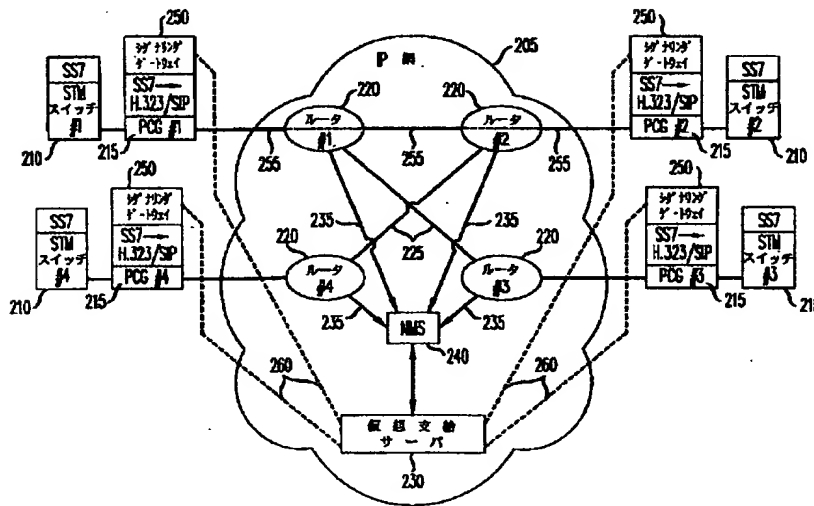
【図4】本発明の一つの実施例において用いられる帯域幅割り当ての構造を示す略図である。

【図5】網内の共通のリンクを共有する複数の仮想プライベート網に対する呼の許可制御のためのルゴリズムの実施例を示す流れ図である。

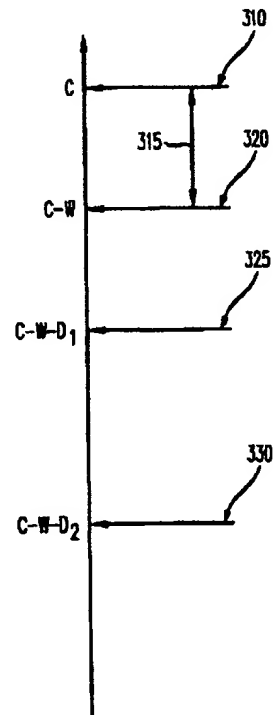
【符号の説明】

- 205 IP網
- 210 STM (Synchronous Transfer Mode) スイッチ
- 215 PCゲートウェイ (Packet Circuit Gateway) エッジデバイス
- 220 ルータ
- 225 物理層ルータ輸送セグメント
- 230 VPサーバ (Virtual Provisioning Server)
- 235 シグナリングチャネル
- 240 網管理システム (Network Management System, NMS)
- 250 シグナリングゲートウェイ (Signaling Gateway)
- 255 網経路
- 270 仮想プライベート網シグナリング経路

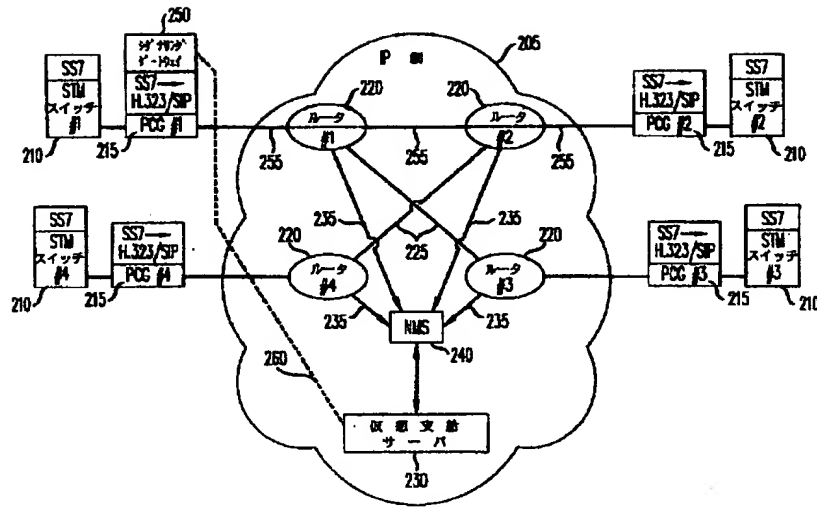
【図1】



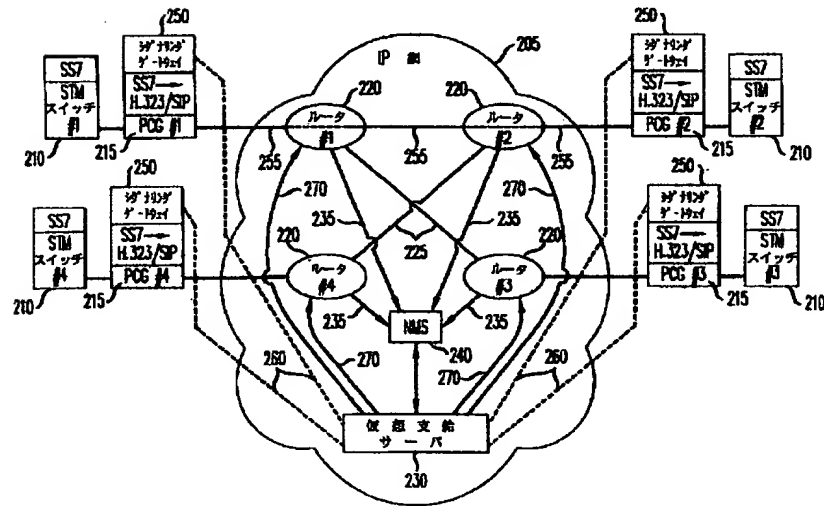
【図4】



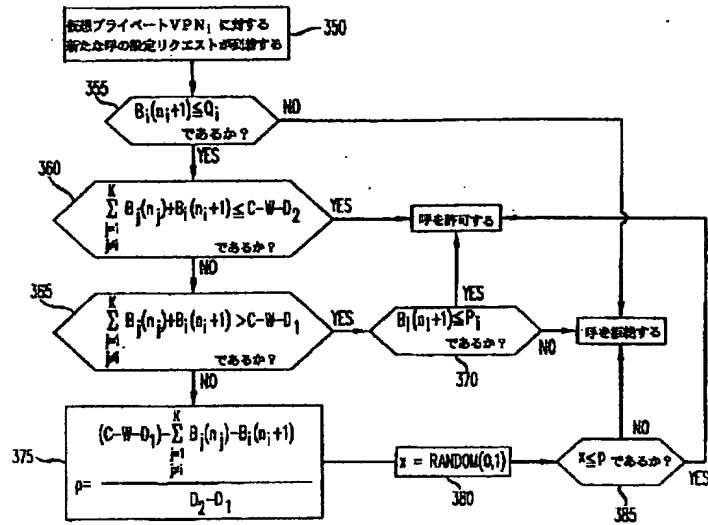
【図2】



【図3】



【図5】



フロントページの続き

(72)発明者 エンリキュー ハーナンデッツ-ヴァレン
シア
アメリカ合衆国 07732 ニュージャーシ
ィ, ハイランズ, ヴァレー アヴェニュー
78

(72)発明者 コチカラアディ スリラム
アメリカ合衆国 07746 ニュージャーシ
ィ, マールボロー, バーリントン ドライ
ヴ 15

(72)発明者 ユン-ターン ワン
アメリカ合衆国 07746 ニュージャーシ
ィ, マールボロー, ピーチ ツリー コー
ト 7

(72)発明者 オン-チン ユエ
アメリカ合衆国 07748 ニュージャーシ
ィ, ミドルタウン, プレヴィンズ アヴェ
ニュー 57

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☒ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.